Sunniva Meyer

PREVENTING MASS KILLINGS: OPTIMAL STRATEGIES FOR PROTECTING PUBLIC TARGETS AGAINST TERRORIST ATTACKS

Dissertation submitted for the Ph.D. degree

Institute of Political Science

Faculty of Social Sciences

University of Oslo

May 2011

Series of dissertations submitted to the
Faculty of Social Sciences, University of Oslo
No. 312

ISSN 1504-3991

Cover: Inger Sandved Anfinsen.
Printed in Norway: AIT Oslo AS.

Produced in co-operation with Unipub, Oslo.
The thesis is produced by Unipub merely in connection with the
thesis defence. Kindly direct all inquiries regarding the thesis to the copyright
holder or the unit which grants the doctorate.

Contents

Abstract

Practitioners with limited security resources lack appropriate guidelines when protecting targets against mass-casualty attacks. Existing guidelines about prioritization between targets and protective security measures are either very abstract or consist of roughly collected advice. Combining game theory with practically oriented literature, such as situational crime prevention, crime scripts and crime prevention through environmental design, this dissertation establishes a systematic framework for prioritizing between targets and measures and provides concrete policy recommendations (given certain assumptions about motivation). I argue that:

1. If terrorists cannot be deterred from attacking, strategic authorities will ensure that the terrorists attack well-protected targets. Protection is desirable not only when it deters the terrorists from attacking, but also when it causes the terrorists to target sites that are less rather than more damaging for the authorities.
2. When protecting against mass-casualty attacks, the authorities should give priority to potential targets with a high expected number of casualties, many foreigners, low employee density, many hiding places, many access points, high anonymity, high share of earlier attacks, and high system fragility.
3. When protecting against explosive attacks on railway networks, the best protective security measures focus on limiting the damage caused by an explosive attack, rather than on reducing the probability of an attack's being successful.
4. By thinking counter-terrorism when designing railway carriages, we may significantly reduce the expected damage caused by explosive attacks on railway.

Many of this dissertation's models generate interesting empirically testable implications. Unfortunately, lack of appropriate data prevents proper testing of these empirical implications as well as testing of assumptions underlying the models; available datasets do not distinguish between attacks where the terrorists seek mass-killings and attacks where they do not. My policy recommendations are, furthermore, less concrete because of the very generic depiction of the terrorists in my models. To refine these recommendations, more knowledge is needed about what resources and capabilities terrorists possess.

Preface

A merge and a funnel. This Ph.D. dissertation can be characterized as both. A merge in the sense that the dissertation merges very distinct traditions, including abstract formal modelling, crime prevention theory and operative advice for security officials. A funnel in the sense that it starts on a very general and abstract level with formal modelling and ends up with developing concrete and narrow advice for designing explosion-resistant railway carriages.

I owe several people and environments gratitude for making this dissertation possible. First, I would like to thank my supervisor, Professor Jon Hovi at the Department for Political Science, University of Oslo, for supporting me (and guiding me) at all crossroads. I am very grateful for you agreeing on supervising me in the first place and for always being there for me when I needed it. I have always been very pleased that I chose you as my supervisor and I would undoubtedly have asked you again.

Second, I would like to thank my managers and colleagues at the Institute of Transport Economics (TØI). I would especially express gratitude to Marika Kolbenstvedt and Torkel Bjørnskau for giving me this Ph.D. opportunity and for their support through this process. I would also like to thank my colleagues at the Department for Safety and Environment for the wonderful social and professional environment they have offered me. You've brightened my days!

Third, I would like to thank Gloria Laycock and all the other people at the Jill Dando Institute of Crime Science (JDI) at University College London for letting me stay and work there in the spring of 2010. I both learned a lot from you guys and had an immensely good time. During my stay, I met several people, both from academia and from the business in general, that have contributed to this project; Paul Ekblom, Aiden Sidebottom, Adrian Dwyer and Toby Davies are only some of them.

Fourth, I would like to thank my former colleagues at the Norwegian Defence Research Establishment (FFI) for comments during this process. I would especially draw attention to the researchers, including Truls Tønnessen and Brynjar Lia, at the TERRA project for informative discussions about terrorists' motivations and calculations behind attacks.

I would furthermore offer thanks to my parents for indirectly contributing to my dissertation. To my mother, Ingrid Synnøve Meyer: I am very grateful for your continous

support during my efforts to find my own professional way. Your support has empowered me to reach for what I really enjoy. To my father, Per Gunnar Frislid: You have throughout my life inspired my academic curiosity. Thank you!

I also want to thank family, friends and other relations for just making my life richer. While I have enjoyed my Ph.D. work, my life is still more about all the other experiences life has to offer; and you guys are a prerequisite for me experiencing them.

Finally, I owe thanks to the Institute of Transport Economics and the Research Council of Norway for funding this dissertation. I am also grateful for the funding of my research stay at the JDI I received from the Ryoichi Sasakawa Young Leaders Fellowship Fund and Ella and Robert Wenzin's Legate.

Sunniva Meyer

Introduction

Background

> Just after the train left Edgware station, there was a massive bang followed by two smaller bangs and then an orange fireball. I put my hands and arms over my ears and head as the windows and the doors of the carriage shattered from the blast. Splintered and broken glass flew through the air towards me and other passengers. I was pushed sideways as the train came to a sudden halt. I thought I was going to die. Horrific loud cries and screams filled the air, together with smoke, bits and chemicals.[1]

In this way, John, a survivor of the 7/7 London attack, describes his experience when the Edgware Road bomb went off. The 7/7 London attack caused 52 killings, approximately 700 injuries (London Assembly, 2006a: 6) and extensive damage to the three trains and the bus targeted in the attack. The track in the three tube locations was also damaged, but no tunnel sections collapsed (Transport for London, 2005b). The tube was totally closed down, causing large transportation problems for everyone travelling in London that day. The day after, all the unaffected lines were reopened, while the Circle and Piccadilly lines were not properly restored until four weeks later (Transport for London, 2005a, 2005c). Except for transport disruption, the economic consequences for businesses were rather small (London Chamber of Commerce and Industry, 2005). Many people, however, suffered from post-traumatic stress (BBC news, 2010), and a significant share of London residents suffered from 'substantial stress' 7 months after the attack (Rubin, et al., 2007).

Mohammad Sidique Khan, the alleged ring leader, describes his motivation for the attack in his video testament (The Stationary, 2006: 19):

> Your democratically elected governments continuously perpetuate atrocities against my people all over the world. And your support of them makes you directly responsible, just as I am directly responsible for protecting and

[1] London Assembly (2006b) p. 4.

> avenging my Muslim brothers and sisters. Until we feel security, you will be our targets. And until you stop the bombing, gassing, imprisonment and torture of my people we will not stop this fight. We are at war and I am a soldier. Now you too will taste the reality of this situation...

In the above extract, Khan explains why he considers all civilians legitimate targets. Many terrorist attacks seemingly aim to produce fear, publicity and indiscriminate mass killings (Al-Hakaymah 2008; Lia 2003; Lia 2008; Tønnessen 2007). The London attackers did not limit the number of killings by notifying the government about the bombings. They furthermore carried the bombs themselves, ensuring that the bombs would not be discovered and rendered harmless before detonation. One of this attack's main *immediate* purposes was accordingly to cause mass-killings, where the immediate purpose of causing mass-killings (and fear) can be interpreted as a means to frighten the population into forcing the politicians to withdraw UK forces from Muslim countries.

Research questions

When securing against terrorism, the authorities must reduce other expenditures correspondingly, for instance, spending on traffic safety, schools or health services. Security resources are thus limited and should be prioritized so as to make the most of them. The purpose of this dissertation is to develop a framework to determine how the authorities should prioritize between both targets and protective security measures when preventing mass-killings. Research questions include:

1. How can we determine whether terrorists consider security measures implemented when selecting targets?
2. How should the authorities prioritize between targets when protecting them against terrorist attacks?
3. How should the authorities prioritize between security measures when protecting the railway against explosive attacks?
4. How should an explosion-resistant railway carriage be designed?

These questions vary from the very general and abstract to the very specific and concrete, which reflects the fact that my dissertation (and writing process) can be characterized as a funnel: Paper 1 discusses question 1; I formulate four abstract models and deduce empirically testable implications from these. Paper 2 answers question 2 building on formal models while also translating abstract implications into concrete policy recommendations. I furthermore compare these policy recommendations with actual allocations in transport. Paper 3 satisfies question 3; here I discuss how to prioritize between concrete security measures in the railway while building on the logic from papers 1 and 2. Paper 4 responds to question 4, discussing the practical problem on how to design an explosion-resistant railway carriage. This dissertation thus consists of four papers, plus the introduction.

Studies in situational crime prevention have shown that different categories of crimes (and terrorism) exist, and that each category should be analyzed separately (Clarke & Newman, 2007). This dissertation focuses on terrorists that attack to achieve some immediate effect[2], where the wanted effect can be killings, material damage, disruption, media coverage etc. I also limit this dissertation to protective security measures, including measures such as passenger screening, target hardening, and closed-circuit television. I ignore measures that are not target specific, such as building and maintaining normative barriers against criminal actions and efforts to hunt down and detain terrorists before or after they have committed violent acts (Bjørgo, 2011). I furthermore focus on economic (and sometimes operational) costs of implementing security measures, ignoring important considerations such as privacy, mobility and other restrictions of freedom.

The framework I develop can be employed to all types of terrorism, but when employing it to produce concrete implications and policy recommendations; I need to restrict the study even further. When necessary, I limit the discussion to mass-casualty attacks because (1) human casualties and serious injuries are extremely expensive for society and (2) the likelihood of casualties and injuries grows when

[2] Terrorists that do not care about the effect of attacking are even more difficult to predict while at the same time probably not as dangerous (they will often choose targets that are too well protected to actually achieve any significant effect).

terrorists actually want to cause mass-killings. What is more, one relatively easy way to attract attention and trigger mass hysteria is to cause large numbers of deaths (Lia 2003: 8).

Public transport constitutes an attractive target for terrorists seeking to cause mass-killings; public transport sites are both crowded and easily accessible. Several of the deadliest attacks in European history have, furthermore, targeted passenger traffic on railways (Lia & Nesser, 2005: 37–38). Railway can thus be an attractive target for terrorists seeking to cause mass-killings by using guns, other small arms, explosives,[3] or unconventional weapons[4] (Clarke & Newman, 2006: 109–110). Explosives are particularly attractive; they can damage structures and bring down buildings, as well as kill people. Furthermore, media coverage of bombings is considerably more graphic than coverage of, say, a shooting (Clarke & Newman, 2006: 109).

Plan for the introduction

Section 2 reviews the literature on prioritization in protective security and shows how this dissertation contributes to this literature. Section 3 discusses this dissertation's research strategy, including the formal models and the empirical analysis, and section 4 four accounts for how the papers relate to each other. Section 5 presents paper summaries, and, finally, section 6 sums up this dissertation's major findings and limitations.

[3] Explosives here include both high explosives and low explosives. See Petropouleas (2009: 3-4) for definitions.
[4] Unconventional weapons include Chemical, Biological, Radiological and Nuclear (CBRN) weapons.

Literature review

The literature on counterterrorism and optimization is vast, ranging from simple risk analysis,[5] where the probability of an attack is exogenous, to game-theoretic models where the protection level influences the probability of an attack. In risk analysis, the probability is usually estimated from the historical frequency of the event (Aven, 1998: 5), a method which is, owing to the relatively low frequency of terrorist attacks, unsuitable for estimating the probability of terrorist attacks. Powell (2007b: 528–530) furthermore demonstrates how using exogenous probabilities against a strategic adversary produces a suboptimal security allocation. Allocating security resources to a site has two effects: it reduces the probability that an attacker will target this particular site and it reduces the probability that an attack on this site will succeed. Simple risk analysis typically includes the second effect, but not the first. Hence, simple risk analysis tends to overestimate the optimal security allocation to the target that is most likely to be attacked when all targets are unprotected.

The above account demonstrates the necessity of considering how terrorists adapt after observing security measures implemented before determining the optimal allocation. The rational choice approach can be an appropriate tool owing to the theoretical coherence, the fruitful simplification[6] and its capacity to explain puzzling outcomes and generate non-obvious solutions (Geddes, 2003: 205). Game-theoretic models are furthermore specifically designed to help us understand the phenomena that we observe when decision-makers interact. Such models assume that decision-makers take into account their knowledge or expectations of other actors' behaviour when pursuing exogenous goals (Osborne & Rubinstein, 1994: 1).

Several scholars have made important contributions to the game-theoretic literature on defender's optimal security allocation (Bier, 2007; Golany, Kaplan,

[5] The risk of an event is the probability of the event multiplied by its consequence.

[6] The restrictive assumptions empower the observer to make deterministic predictions about behavior. Geddes (2003: 189-90) illustrates this by comparing rational choice arguments with if-then statements: "if the actors have the goals the observer claims, and if the information and calculation requirements are plausible (…), and if the actors actually face the rules and payoffs the observer claims they do, then certain behavior will occur."

Marmur, & Rothblum, 2009; Hausken, 2006; Powell, 2007a, 2007b, 2008; Sandler & Lapan, 1988). Bier (2007) and Powell (2007b, 2008) analyze the optimal security allocation when the defender has full information about the attacker's preferences. They demonstrate that, up to a point, it is optimal for the defender to allocate all its security resources to the site the attacker most prefers to target. When the defender has invested enough resources at the attacker's most-preferred target to make the attacker indifferent between targeting the two most-preferred sites, then the defender should divide the next resources equally between these two targets. When the attacker becomes indifferent between targeting the three most-preferred sites, the defender should divide the next resources equally between these three targets, and so on.

Defender's optimal strategy might, however, be different if the defender can withhold information about the allocation. Zhuang and Bier (2007) model the defender's use of secrecy. Their analysis shows that when full information exists about the defender's preferences, the defender always prefers to reveal the security allocation truthfully. However, when the defender has private information, certain situations exist where secrecy and/or deception may be preferred by the defender to mimic a defender that are of less interest to the attacker.

Powell (2007a) shows that when only the defender is aware of the targets' vulnerability (the probability of an attack on each target succeeding), the allocation of security resources to the targets may be treated as signals about the sites' vulnerabilities. The need for secrecy about vulnerability overrules the need for securing vulnerable targets when sites that are more vulnerable are slightly harder to protect "on the margin". The defender may therefore divide its resources equally, regardless of the vulnerability level.

The above game-theoretic literature on defender's optimal security allocation have interesting implications, but most so at a very general and abstract level. Authorities working on target protection need more concrete advice, advice that can be found in the more practically oriented literature I account for below.

"Security is deliberate action to reduce the risk of criminal events, taken before, during or after the event" (Ekblom, 2011: 97). Societies have been implementing security measures for all known history, measures that do anything from dealing out punishment to offenders to building walls to keep potential offenders away. Security can be further refined into four distinct approaches (Ekblom, 2011: 97):

1) Primary security either eliminates the possibility of an unwanted event or reduces the probability that such an event will happen. An example is passenger screening to decrease the probability of an explosive being smuggled into a target area.
2) Secondary security limits harm if the unwanted event occurs. An example is installing blast-resistant glass that does not form damaging fragments in an explosion.
3) Tertiary security limits propagation of harm that may occur post-event. An example is use of fire-resistant materials in the carriages' inventory to prevent fires ignited by an explosion.
4) Mitigation attempts to repair the harm that has already been done. An example is rebuilding damaged buildings after a successful attack.

This dissertation focuses on target-specific security measures implemented before the criminal event, namely 1–3.

The situational crime prevention approach focuses on specific crime categories and seeks to change the immediate environment, such that potential offenders either are physically prevented from committing the crime or perceive the opportunities as reduced and the risk as increased, and thus might choose against committing the specific crime (Clarke, 1983: 225; Ekblom, 2010). Clarke and Newman (2006: 189–195) apply situational crime prevention measures for protecting targets against terrorism, including explosive attacks. They propose: increasing the effort by closing off streets and building walls and barriers; increasing the risks of being caught by strengthening surveillance through CCTV, citizen vigilance and hotlines; and reducing the offender's rewards by making the buildings more explosive-resistant and designing public spaces to reduce injuries from bombs.

Crime Prevention through Environmental Design (CPTED) specifically emphasizes the process of designing security into the built environment/architecture (Atlas, 2008: 3). Contributors concentrate on physical measures against explosive attacks in general (Atlas & DiGregorio, 2008; FEMA, 2003, 2007, 2008; Garcia, 2008; Petropouleas, 2009). CPTED-measures include everything from measures preventing progressive structural collapse (incorporating more columns in the design, strengthening floor systems, strengthening un-reinforced masonry walls and shaping the buildings optimally) (FEMA, 2008: 3-23 to 3-29), via measures preventing damage from fragments (glazing, securing walls, securing non-structural debris and other facade retrofits) (FEMA, 2008: 3-10 to 3-23), to measures facilitating evacuation (designing good evacuation routes, signing them clearly and installing emergency lighting).

The above contributions provide many excellent suggestions for security measures, while mostly ignoring the implementation cost. A few contributors acknowledge that authorities have limited resources available: If the standoff is large and vehicles cannot approach the premises, the need to secure against structural collapse in case of a vehicle-borne explosive attack decreases and vice versa. The optimal trade-off between standoff and structural robustness depends on the price per square metre (Petropouleas, 2009). Increasing blast resilience is furthermore much cheaper when implemented in the design phase than when implemented later (Aibara, 2010).

Other contributors suggest relatively cheap measures. Since nine out of ten deaths in explosions are caused by flying glass (Phillips, 2010), measures that prevent glass fragmentation is a relatively cheap way of reducing the number of injuries caused by an explosion. Intelligent use of people that already frequents the transport system are furthermore a relatively cheap way of enhancing security, training of both security personnel and civilian staff, and support of passenger vigilance (Jenkins, 2001: 14–17). In the UK railway's strategy for dealing with unattended items, passengers are told specifically to keep their belongings with them and report to a staff member when seeing anything unattended. The front line staff is trained to employ the 'HOT'

protocol[7], and police officers receive both training and regular intelligence updates (Dwyer, 2010: 6–7).

In summary, there is a huge gap in the literature between very formal game theoretic contributions that have precise, but very abstract implications, and the more hands-on contributions that largely produce ad hoc advice. This dissertation aims to bridge this gap by combining formal theory, such as the above game-theoretic literature, with more practically oriented contributions, such as the situational crime prevention approach, to produce concrete policy recommendations for relevant authorities.

[7] HOT stands for: is the item Hidden? Is it Obviously suspicious in appearance or placement? Is it Typical of lost property? (Dwyer, 2010: 21)

Research strategy

This dissertation encompasses four papers, all which apply formal models, directly or indirectly, to generate concrete policy recommendations for authorities securing targets against terrorist attacks. Paper 1 employs four models to investigate target selection by terrorists and to deduce empirically testable implications. Paper 2 employs two of these models to explore how the authorities should allocate security resources between targets. I deduce implications and translate them into policy recommendations that are compared to data collected through interviews with Norwegian transport authorities. Paper 3 applies one of the above models to prioritize between security measures against explosive attacks in railway networks. Paper 4 combines the reasoning from paper 3 with the language of the so-called Security Function Framework to explore the specific practical design problem of securing railway carriages against explosive attacks.

Formal models

Why use formal models? According to Snidal (2004: 227) "mathematics provides a precise language to describe the key elements of a problem, a powerful deductive machinery that extends the logical power of our theories, and an important means to expand our understanding and interpretation of the world." Employing mathematics thus both clarifies and facilitates deduction from a theoretical argument. Mathematics has, however, also limitations; formal modelling often requires restrictive assumptions, assumptions which must be properly justified in each case.

All this dissertation's models can, to varying degrees, be characterized as rational choice models. Rational choice models use the individual, or some analogue of the individual, as the unit of analysis and treat the individual's goals as exogenously given. They furthermore assume that individuals, given their knowledge about strategies, costs and benefits, select the alternative that maximizes their expected utility. Structural characteristics determine the set from which individuals may

choose their strategies and the costs and benefits associated with each strategy (Geddes, 2003: 179).

Rational choice arguments suffer, however, from some limitations. A good rational argument depends on both the goals' plausibility and the analyst's ability to identify these goals a priori. According to Geddes (2003: 180–1), rational choice argument tends to be less persuasive when the goals are more idiosyncratic. When the actors have unusual goals, exploring the origin of these goals can be more interesting than constructing a rational choice argument which explains the behaviour given these goals. She furthermore claims that goals should not be directly inferred from observed behaviour because the rational choice argument then turns into mere tautology (Geddes, 2003: 181).

I actually use rational choice arguments to explore behaviour by individuals with rather idiosyncratic goals, terrorists. Other scholars focus, however, on understanding the ideologies behind terrorist behaviour, such as jihadism, and/or focus on terrorist recruitment[8]. Terrorism has such high impact that, even if it is characterized as a rather marginal phenomenon, exploring the behaviour seems useful.

Two of this dissertation's models are game theoretic. The distinctive feature of game-theoretic models is "that actors are interdependent so that each actor's outcome depends in part on the other's behaviour" (Snidal, 2004: 247). Kydd (2004: 346) claims that the field of security studies is especially suited for game theory. The number of actors is usually small and the stakes involved are high. Practitioners of world politics, furthermore, often have extensive experience with the relevant issues (Kydd, 2004: 347–8). Is game theory suitable for studying terrorism? The number of possible terrorist cells is obviously vast and, as shown in paper 2, the authorities do not act like a unitary actor. However, modelling terrorism as a game between a terrorist cell and the authorities is fruitful when the purpose is generating policy recommendations for the authorities. The actors consider the outcome important; the authorities want to minimize mass-killings and, since the terrorists may not get a

[8] See for instance Hegghammer (2006) and Lia (2008).

second chance (because they can either be killed in the attempt or have high risk of being caught), the terrorists want to maximize the effect of the attack, including causing mass-killings. Few authorities and terrorists, however, have lots of experience with terrorism. Few states have experienced terrorist attacks and very few terrorists stay free to commit new attacks after committing serious terrorist attacks in Western countries. The main argument against using game theory on terrorism is thus many actors' lack of experience.

This dissertation's models

In this section I discuss the purpose of this dissertation's models.

This dissertation analyzes six different models, of which paper 1 considers four. In model I both the authorities and the terrorists act strategically. Strategic authorities seek to minimize damage from mass-casualty attacks while taking into account how implemented security measures affect both the terrorists' choice of target and their investment in an attack. Strategic terrorists, in selecting their target and attack investment, seek to maximize casualties, given the security measures implemented by the authorities. In model II only the terrorists act strategically, meaning that the terrorists' choice of target and attack investment depends on how the authorities protect the various sites, while the authorities ignore the terrorists' target selection process when allocating security measures. Finally, in models III and IV the terrorists do not act strategically; they simply select the targets likely to have the maximum number of casualties without considering how the authorities' security measures affect the probability that the attack will succeed. In model III the authorities minimize damage while taking into account that the terrorists do not act strategically, while in model IV the authorities ignore the terrorists' target selection and attack investment processes when allocating security measures.

Because paper 2 aims to establish what influences the authorities' optimal security allocation (rather than the terrorists' target selection, as in paper 1), it ignores the cases where the authorities act non-strategically. Furthermore, in paper 2 paper 1's models I and III are replaced by models V and VI to better suit paper 2's purpose.

Unlike models I and III, models V and VI treat the probability of an attack's being successful as independent of the cost of attacking (the attack investment). Model V resembles model I, but treats the cost of attacking as exogenously given and constant across targets. Like model III, model VI assumes that only the authorities act strategically and that Nature (chance) decides with exogenous probabilities the terrorists' choice of target. In model VI these exogenous probabilities vary between 0 and 1. In contrast, in model III they are either 0 or 1.

Table 1 categorizes the six models according to whether the authorities and the terrorists are assumed to be strategic or non-strategic.

Authorities / Terrorists	Strategic	Non-strategic
Strategic	Model I Model V	Model II
Non-strategic	Model III Model VI	Model IV

Table 1: The six models

Models as normative standards

Many formal models are based on unrealistic assumptions about how the actors act (Hovi & Rasch, 1996: 114–6). These models set a normative standard for the actors, rather than describing their actual behaviour.

Four of the models I consider can be seen as normative standards for how the authorities should act. Models I, III, V and VI all assume that the authorities act like a unitary and rational actor to minimize casualties. Interviews with Norwegian transport authorities actually indicate that they neither act like a unitary actor nor allocate resources purely to minimize casualties; other non-security considerations

contribute heavily to the aggregate allocation. These four models should thus be interpreted as normative standards for the authorities.

To aid the authorities when protecting targets against mass-casualty attacks, I explore target selection by terrorists. An adverse effect of this exploration, very difficult to avoid, is that I also establish how the terrorists should act. Models I, II and V assume that the terrorists also act like a unitary actor while maximizing benefit given available information. Whether these assumptions are realistic or not, models I, II and V demonstrate how the terrorists can maximize utility. These models could thus also be interpreted as normative standards, although only for effect-seeking terrorists.

Consequently, models I, II, III, V and VI can be seen as normative standards, either for only the authorities (models III and VI), or for only the terrorists (model II), or for both (models I and V).

Models as conceptual explorations

Some models do not support any claim about the real world; they focus on 'conceptual exploration' rather than 'empirical theorizing' (Sugden, 2000: 9). The scholar investigates the model's internal properties without considering its empirical relevance. Even if the ultimate purpose of model-building is to learn about the real world, conceptual explorations can be valuable; they can improve existing theory by either (1) establishing simpler formulations, (2) discovering useful theorems within these theories, or (3) discovering inconsistencies. Additionally, a model can sometimes explain empirical phenomena in completely different domains than the scholar had in mind when developing the model (Sugden, 2000: 8–10).

This dissertation's models, especially models I and V, rely heavily on existing game-theoretic contributions while simultaneously extending this literature by varying assumptions about strategic behaviour. In addition to the game-theoretic models where both actors act strategically (models I and V), I consider one model where the terrorists are assumed to act strategically while the authorities' allocation

of resources is non-strategic (model II), two models where only the authorities act strategically (model III and VI), and one model where both actors act non-strategically (model IV). I furthermore deduce implications about terrorists' target selection or the authorities' optimal security allocation from all six models and compare these implications. I thus show how both terrorists' target selection and the authorities' optimal allocation depend on the assumptions about strategic behaviour. These models can thus be called interesting conceptual explorations.

Models as instruments

How can unrealistic models explain real-world phenomena? Instrumentalists argue that a model "should be judged only on its predictive power within the particular domain in which it is intended to be used" (Sugden, 2000: 11). Theories cannot be true or false and are thus not to be understood literally. Theories "are tools or calculating devices for organizing description of phenomena, and for drawing inferences from the past to future" (Hacking, 1983: 63). When a model is used instrumentally, it should generate empirical implications that are clearly distinct from its assumptions (Sugden, 2000: 12).

All the formal models in this dissertation separate clearly between assumptions and implications. The assumptions are listed in the model descriptions and the implications are deduced from the equilibria. I deduce several implications from each of the models. Consequently, it is reasonable to maintain that the formal models are valuable in the instrumentalist sense if their implications survive empirical evaluation. Unfortunately, as mentioned in section 3, lack of appropriate data of high enough quality has made it impossible to test the models' implications. The models are thus in principle valuable as instruments owing to producing implications that are falsifiable. This conclusion is, however, tentative since the implications have not survived an empirical evaluation.

Models as credible worlds

Assuming that researchers aim at finding the truth about the world, it makes sense to ask whether the models are good descriptions of the world. But in what way may the models be good descriptions of the world? Gibbard and Varian emphasizes explanation rather than prediction. In their view, a model either explains an empirical phenomenon, or investigates the likely consequences of a real-world phenomenon. The model's purpose is to communicate this explanation, or the likely consequences, to an audience (Sugden, 2000: 12–3). Gibbard and Varian furthermore suggest that models are caricatures. The model's assumptions should thus be selected "not to approximate reality, but to exaggerate or isolate some feature of reality" (Gibbard & Varian, 1978: 676). Mäki claims that economic scholars employ the method of isolation when formulating models: "a set of elements is theoretically removed from the influence of other elements in a given situation" (Mäki, 1992: 318). The effects that the theory wants to describe are isolated, and all other influences are sealed off. The method of theoretical isolation parallels the idea of experimental isolation. In experiments all other influences than the object of the study are sealed off. Theoretical isolations, or models, can thus be called *thought experiments* (Sugden, 2000: 15).

But how can thought experiments, which rely on restrictive assumptions, tell us something about the real world? Sugden (2000: 19) explains that the transition "from a particular hypothesis, which has been shown to be true in the model world, to a general hypothesis, which we can expect to be true in the real world too," should be made through inductive inference. He then claims that for a model to be credible enough to justify inductive inference, the assumptions need to cohere with both each other and "with what is known about causal processes in the real world" (Sugden, 2000: 26). The assumptions can be restrictive, but they must also seem adequately representative for the real world.

Models I, III, V and VI in this dissertation does not seem realistic. Interviews with Norwegian authorities indicate that they do not act like a unitary rational actor when allocating security resources. These models are thus not credible worlds. Models II

and IV might, however, be more realistic; both assume that the terrorists attempt to maximize their subjective benefit of the attack without suffering too large subjective cost. Model II also assumes that the terrorists consider implemented security measures before choosing a target while model IV assumes that the terrorists ignore the security allocation. Depending on whether any of these assumptions seem credible, models II and IV might be considered reasonably good descriptions of the world.

Models as fables

Rubinstein (2006) presents an alternative, more austere, perspective on models. He claims that some formal models are unrealistic in the sense that they can lead to absurd conclusions, someone will nearly always be able to find an experiment to defeat the model and very few models can be used to provide serious advice. Models are furthermore not always necessary to find interesting regularities. He then claims that a good model resembles a good fable in the sense that, even if unrealistic, it draws a highly simplified parallel to a real-life situation, is free of extraneous details, and conveys some sound advice or relevant argument that can be used in the real world (Rubinstein, 2006: 881). Rubinstein states that "as in the case of a good fable, a good model can have an enormous influence on the real world, not by providing advice or by predicting the future, but rather by influencing … the way people think and behave" (Rubinstein, 2006: 881).

Can this dissertation's models be interpreted as fables? The models draw a parallel to a situation in real life: the processes of terrorists' selection of targets and authorities' allocation of security resources. All the models are furthermore free of extraneous details; they ignore, for instance, any deliberations before the players act. Finally, models I, III, V and VI convey advice (policy recommendations) to the authorities for use in the real world. Models II and IV also present relevant arguments for use in the real world; they explore how the terrorists might behave when the authorities ignore the terrorists' behaviour.

This dissertation's models can thus also be interpreted as fables.

Summary

The above discussion is summarized in table 1.

Models as…	Normative standards	Conceptual explorations	Instruments	Credible worlds	Fables
Model I	X	X	X		X
Model II	X		X	X	X
Model III	X		X		X
Model IV			X	X	X
Model V	X		X		X
Model VI	X		X		X

Table 2: The discussion summarized

This section has explained how this dissertation's models can inform us about the real world. Models I, II, III, IV, V and VI set a normative standard for behaviour: models I, III, V and VI explain how the authorities should act and models I, II and V show how terrorists should behave (given their goals). The anthology of models, furthermore, constitutes a conceptual exploration. In addition, all the models distinguish between assumptions and implications and can thus be described as (untested) instruments. Models II and IV might also be good descriptions of the world. Finally, all the models can be interpreted as fables.

Empirical analysis

In paper 2 I compare implications deduced from the models with empirical data. The paper, however, suffer from a shortage of relevant data and I, thus, cannot perform any proper test of the implications/policy recommendations.

To examine the behaviour of the multiple Norwegian transport authorities, I interviewed authorities responsible for protection of public transport targets. I conducted fourteen semi-structured interviews, seven in person and seven by phone. I selected organizations I consider representative for each of the transport modes (aviation, shipping, railway and public road transport). In aviation and railway I attempted to get an interview with 3–4 of the largest authorities in each mode that I believed were responsible for target protection. However, in shipping and public road transport, I had to make a selection of 4–5 authorities owing to the vast number of actors. Three interviewees declined: One scheduled interview with a company serving a ferry line in Norway and overseas was replaced by an interview with a similar ferry company. The other two interviewees who declined were unfortunately not replaceable. However, I interviewed authorities that regularly interact with these companies. These interviews indicated that other authorities than the missed companies in the transport mode were primarily responsible for target protection. Consequently, I have assumed in my analysis that the missed authorities do not spend anything on target protection measures. Even if this assumption may not be strictly true, I believe the actual spending is so small that the error is very small at worst.

Of course, deciding whether the actual allocation is optimal is impossible without looking at the actual allocation. When I interviewed the Norwegian authorities responsible for the protection of public transport targets, I also collected information about *the amount of security resources*[9] *allocated to target protection*[10]. I have tried to establish for what purpose these resources were allocated. I have included all the

[9] The allocation is measured in Norwegian kroner.

[10] The amount of security resources allocated to target protection may not reflect the overall security level. The security level also depends on security culture and security procedures that do not generate extra spending.

time spent on risk analysis, planning, knowledge transference and rehearsing for security; I have collected information about the number of man-labour years used and calculated the expenditures, assuming that the cost of a man-labour year is 1.2 million Norwegian kroner. In some cases, the only spending on security actually was the time spent every five years or so on planning for a terrorist event. In these situations I calculated the amount of time spent on planning each time and divided it on the number of years the plan should last. Some security spending has been excluded; the expenditures on guarding have not been included when measuring the amount of security resources allocated to railway stations and bus terminals. The large number of security guards on some of the largest nodes is caused by the high amount of crime and misconduct, and the same number of guards would likely have been employed even without any threat whatsoever from mass-casualty attacks. Decomposing the expenses into allocations to specific targets, for example to specific railway stations, proved too difficult. I have therefore collected information about expenditures from representative authorities in each transport mode. Consequently, the data do not reflect the differences in security expenditures within each transport mode (aggregation problem). Furthermore, if the authorities interviewed are less representative than I assumed, the data may be biased.

Owing to the small number of cases and the abovementioned aggregation problem, paper 2 cannot offer any proper test of the models' implications. The interviews do, however, show that it is unlikely that the authorities allocate security resources optimally in the sense that they minimize the number of casualties and the transport disruption.

The relationship between the papers

All the papers in this dissertation share a primary purpose: advising the authorities about protecting targets against terrorist attacks (even if indirectly through designers). They furthermore build on the same research strategy, applying formal models to deduce concrete implications which can be, and to some extent are, confronted with empirical data. This strategy is very explicit in papers 1 and 2, while more implicit in papers 3 and 4; paper 3 builds on model I in papers 1 and 2 while paper 4 builds on the reasoning from paper 3.

The papers differ in at least three respects. First, paper 1 focuses on terrorists' behaviour; all implications predict how terrorists behave under different assumptions. In contrast, papers 2 and 3 focus on the authorities, by deducing policy recommendations for prioritization between targets and measures when protecting targets against terrorist attacks. Paper 4, furthermore, focuses on how the designer should deal with the specific practical design problem of securing railway carriages against explosive terrorist attacks.

Second, the papers differ concerning which parameters are treated as exogenous and thus constant. Papers 1 and 2 assume that the authorities can only influence the probability of an attack's being successful. Papers 3 and 4, in contrast, assume that the authorities can also influence the impact of a successful attack and the terrorists' cost of attacking.

Finally, the papers differ in their technical level. The theoretical parts of papers 1 and 2 are very formal in structure and a relatively high level of technical skill is required to understand all parts. In contrast, the theoretical parts of papers 3 and 4 are more accessible.

Paper summaries

The first paper explores terrorists' choice of target when attacking. Some scholars argue that if one site is secured, terrorists will simply attack a different site (target substitution). Other scholars claim that terrorists do not care whether their attack succeeds; they focus on committing the act. Assuming that terrorists seek some sort of immediate effect from attacking, this paper derives empirically testable implications from four different formal models. Investigating the correlation between the authorities' security allocation and the terrorists' target selection enables us to distinguish between strategic and non-strategic authorities and terrorists. Strategic authorities implement security measures to minimize damage from terror attacks, taking into account how these measures affect the terrorists' target selection and their investment in an attack, while non-strategic authorities allocate security resources based on other factors than expected utility. Strategic terrorists select targets and attack investment to maximize effect, taking into account implemented security measures, whereas non-strategic terrorists ignore implemented security measures.

I demonstrate that if terrorists cannot be deterred from attacking, strategic authorities will ensure that the terrorists attack well-protected targets. Protection is desirable not only when it deters the terrorists from attacking, but also when it causes the terrorists to target sites that are less rather than more damaging for the authorities.

The second paper explores the optimal allocation of protective security resources between targets given different assumptions about terrorists' target selection. The paper defines the optimal allocation as the allocation that minimizes expected casualties. Few scholarly contributions on allocation of security resources offer concrete policy recommendations. I contribute towards closing this gap by (1) translating theoretical notions of optimal security allocations into concrete policy recommendations and (2) comparing these recommendations with actual Norwegian security allocations in transport. I argue that, when protecting against terrorist attacks, priority should be given to potential targets that display a high expected number of casualties, many foreign travellers, low employee density, many hiding

places, many access points, high passenger anonymity, high share of earlier attacks and high system fragility. Interviews with Norwegian transport authorities suggest that international commitments and each authority's budget constraints, rather than concerns for efficiency at the aggregate (national) level, determine the authorities' allocation of security resources.

The third paper assumes that a main goal of the authorities is to minimize human casualties and injuries. It explores which measures should be prioritized when protecting a railway network against explosive attacks. The literature on protective security measures against terrorism focuses mainly on suggesting measures for protecting targets rather than on prioritizing between measures. This paper attempts to bridge this gap by combining game theory with lessons from situational crime prevention theory, crime scripts and crime prevention through environmental design to prioritize between protective security measures against explosive attacks on railways. The discussion shows that measures that focus on limiting damage caused by the explosive attack rather than measures that reduce the probability of the attack's being successful are the best protective security measures. This paper argues that the best protective security measures have a huge effect on the expected harm of explosive attacks compared to cost in currency and operability.

Anyone trying to devise counter-terrorist designs for railway carriages faces a range of issues. In particular, designers need a framework for thinking about security. The fourth paper (co-authored with Paul Ekblom) explores the specific practical design problem of securing railway carriages against explosive terrorist attacks and assesses the benefits of articulating such exploration through the use of the Security Function Framework (SFF). We present the SFF framework, apply it to the ExRes carriage and evaluate it according to defined criteria. Our evaluation shows that the SFF framework is clearly expressed, aids the designer in communicating design requirements, facilitates systematic creativity without necessarily generating completely new ideas, and appears practically applicable. However, we emphasize that ours have been 'bench tests'; such tests are really no substitute for trying the SFF out with real life designers.

Major findings and final remarks

Recent high-profile terrorist events, including the September 11 attack, have led to an enormous increase in the allocation of security resources in the Western World, particularly in public transport. The amount of resources we can spend on security is, however, limited. When spending more on security, the authorities must reduce other expenditures correspondingly, for instance, spending on traffic safety, schools or health services. Security resources are thus limited and should be prioritized so as to make the most of them. Practitioners with limited security resources lack appropriate guidelines when protecting targets against mass-casualty attacks. Existing guidelines about prioritization between targets and protective security measures are either very abstract or consist of roughly collected advice. Combining game theory with practically oriented literature, such as situational crime prevention, crime scripts and crime prevention through environmental design, this dissertation establishes a systematic framework for prioritizing between targets and measures and provides concrete policy recommendations (given certain assumptions about motivation). I argue that:

1. If terrorists cannot be deterred from attacking, strategic authorities will ensure that the terrorists attack well-protected targets. Protection is desirable not only when it deters the terrorists from attacking, but also when it causes the terrorists to target sites that are less rather than more damaging for the authorities.
2. When protecting against mass-casualty attacks, the authorities should give priority to potential targets with a high expected number of casualties, many foreigners, low employee density, many hiding places, many access points, high anonymity, high share of earlier attacks, and high system fragility.
3. When protecting against explosive attacks on railway networks, the best protective security measures focus on limiting the damage caused by an explosive attack, rather than on reducing the probability of an attack's being successful.

4. By thinking counter-terrorism when designing railway carriages, we may significantly reduce the expected damage caused by explosive attacks on railway.

These policy recommendations should ideally have been tested. Testing is, however, very difficult owing to both lack of appropriate data and costs of experiments. Datasets that are large or detailed enough to do proper quantitative or qualitative testing are wanting, and even experiments that only test one specific measure can be extremely expensive to carry out, e.g. blowing up structures to investigate what strengthens structural redundancy. Testing the recommendations are thus outside this dissertation's scope. Further research should nevertheless aim at evaluating the recommendations when feasible.

Since testing the policy recommendations are outside this dissertation's scope, evaluation of the policy recommendations must assess how they have been derived. This dissertation has formulated several formal models, deduced implications and, by including additional assumptions, translated these implications into policy recommendations. The additional assumptions include: (1) the existence of many hiding places increases the likelihood of an unwanted item being left undisturbed (see paper 2), (2) increased standoff will usually lead to fewer injuries of an explosive attack (see paper 3), and (3) a reduced number of forgotten items will facilitate the discovery of actual left explosives (see paper 4). Since the policy recommendations rely on these assumptions, I have tried to substantiate them when relevant in the papers.

The formal models I deduce implications from are not observable as such and thus not testable. They rest, however, on their assumptions, assumptions which I discuss in the remainder of this section.

This dissertation assumes that the authorities' main aim is to minimize casualties and serious injuries. If the authorities primarily seek something else, the recommendations will probably not apply. If, for instance, the authorities basically seek to increase passengers' sense of safety, rather than their real safety, measures that make the public feel safe will be better than the measures advocated by this dissertation's policy recommendations. Hence, this dissertation's policy

recommendations are only valid if the authorities primarily want to minimize casualties and serious injuries.

Parts of this dissertation (see especially policy recommendations A and B in paper 2) assume that the terrorists primarily seek to cause mass-killings. I do not assume that causing mass-killings is their only goal, nor their long-term goal, only their primary short-term goal. I, furthermore, do not claim that all terrorists seek indiscriminate mass-killings; most terrorist attacks seemingly have other main purposes, such as assassinations and most hostage situations. Statements made by jihadist ideologues and jihadist attackers, however, support the notion that some of these attackers deliberately seek indiscriminate mass-killings. The scope of this dissertation is to formulate policy recommendations that aid authorities in minimizing mass-killings from these attacks.

This dissertation furthermore assumes that the terrorists, at the time of their decision, possess knowledge about (1) all possible targets and modi operandi, (2) the probability of an attack's being successful (if not especially noted that they lack such knowledge), (3) the benefit from a successful attack and (4) their cost of attacking. This knowledge requires both a prior knowledge base and the ability to collect additional information, each which entails analytical abilities, resources (internet, car, etc) and time, any of which they might lack. Some security measures are, furthermore, easy to detect while others might be nearly impossible to discover before actually attacking. For measures that are neither completely public nor completely hidden, there will probably be a time lag between when it is introduced and when the terrorists discover its existence. Reconnaissance before attacking without being detected has also become more difficult lately owing to increased surveillance and larger general awareness about the risk of terrorist attacks. Consequently, the information available to attackers before choosing a target and a modus operandi is limited. The attackers might thus suffer from bounded rationality and as a result copy other successful attacks rather than weigh the costs and benefits of each attack. Such a copy cat strategy would make this dissertation's policy recommendations less valid.

The copy cat strategy, however, actually makes the authorities' job of minimizing mass-killings easier; if the authorities study what other attackers have done successfully (or nearly successfully) and find measures that would have stopped or limited the damage from such attacks, the authorities can implement these measures provided they have the necessary resources available. Furthermore, the authorities can avoid spending security resources on targets that potential attackers lack knowledge about.

Terrorist recruits come from different backgrounds and thus have different prior experience. Such differences might cause divergences in the expected utility of attacking; if a recruited terrorist has some specific knowledge that can be employed when attacking a specific target and/or using a specific modus operandi, it might be optimal for that terrorist to choose that target and/or that modus operandi (because it increases the probability of the attack's being successful). The formal models in this dissertation depict the terrorist only as a seeker of some effect; they ignore how the probability of success might depend on the terrorist's prior experience. The very generic depiction of the terrorist makes the policy recommendations less concrete. This problem can unfortunately not be mended without more knowledge about who is recruited and what sort of background they have.

References

Aibara, D. (2010). Blast Resilience - from strategy to delivery. In NaCTSO (Ed.), *Counter Terror Expo 2010. Protecting Crowded Places Against Terrorism*. National Hall, Olympia.

Atlas, R. I. (2008). What, Me Worry? In R. I. Atlas (Ed.), *21st Century Security and CPTED* (Vol. 1, pp. 3–8). Boca Raton: Taylor and Francis Group.

Atlas, R. I., & DiGregorio, T. (2008). Designing for Explosive Resistance. In R. I. Atlas (Ed.), *21st Century Security and CPTED. Designing for Critical Infrastructure Protection and Crime Prevention*. Boca Raton: Taylor & Francis Group.

Aven, T. (1998). *Pålitelighets- og risikoanalyse*. Oslo: Universitetsforlaget.

BBC news. (2010). 'London bomb stress' recognised (Vol. 2010). London: BBC.

Bier, V. M. (2007). Choosing What to Protect. *Risk Analysis, 27*, 607–620.

Bjørgo, T. (2011). Strategier for forebygging av terrorisme. In T. Bjørgo (Ed.), *Forebygging av terrorisme og annen kriminalitet*. Oslo: Politihøgskolen.

Clarke, R. V. (1983). Situational Crime Prevention: Its theoretical basis and practical scope. *Crime and Justice, 4*, 225–256.

Clarke, R. V., & Newman, G. R. (2006). *Outsmarting the terrorists*. Westport: Praeger Security International.

Clarke, R. V., & Newman, G. R. (2007). Situational Crime Prevention and the Control of Terrorism. In O. Nikbay & S. Hancerli (Eds.), *Understanding and Responding to the Terrorism Phenomenon: A Multi-dimensional Perspective* (pp. 285–297): IOS Press.

Dwyer, A. S. (2010). Intending to travel. Benefit, cost, and the active management of terrorism-related risk in the railway environment. British Transport Police.

Ekblom, P. (2010). Comments on an essay on mitigating harm from explosive attacks in general. In S. Meyer (Ed.). London.

Ekblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5Is Framework*. Basingstoke: Palgrave Macmillian.

FEMA. (2003). Reference Manual to Mitigate Potential Terrorist Attacks against Buildings. *Risk Management Series*. Washington, D.C: Federal Emergency Management Agency.

FEMA. (2007). Site and Urban Design for Security. *Risk Management Series*. Washington, D.C: Federal Emergency Management Agency.

FEMA. (2008). Incremental Rehabilitation to Improve Security in Buildings. *Risk Management Series*. Washington, D.C: Federal Emergency Management Agency.

Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann.

Geddes, B. (2003). *Paradigms and Sand Castles: Theory Building and Research Design in Comparative Politics*. Ann Arbor: The University of Michigan Press.

Gibbard, A., & Varian, H. R. (1978). Economic Models. *Journal of Philosophy, 75*, 664–677.

Golany, B., Kaplan, E. H., Marmur, A., & Rothblum, U. G. (2009). Nature plays with dice - terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research, 192*, 198–208.

Hacking, I. (1983). *Representing and intervening. Introductory topics in the philosophy of natural science*. Cambridge: Cambridge University Press.

Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*, 629–665.

Hegghammer, T. (2006). Terrorist Recruitment and Radicalization in Saudi Arabia. *Middle East Policy*.

Hovi, J., & Rasch, B. E. (1996). *Samfunnsvitenskapelige analyseprinsipper*. Bergen: Fagbokforlaget.
Jenkins, B. M. (2001). Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview. San Jose: Mineta Transportation Institute.
Kydd, A. (2004). The Art of Shaker Modeling. In D. F. Sprintz & Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases. Methods for Studying International Relations*. Ann Arbor: The University of Michigan Press.
Lia, B. (2008). Doctrines for Jihadi Terrorist Training. *Terrorism and Political Violence, 20*, 518 – 542.
Lia, B., & Nesser, P. (2005). Terror mot jarnvegar: Eit oversyn over typiske terroraksjonar mot togpassasjertransport. Kjeller: FFI.
London Assembly. (2006a). Report of the 7 July Review Committee. London.
London Assembly. (2006b). Report of the 7 July Review Committee. Volume 3: Views and information from individuals. London: Greater London Authority.
London Chamber of Commerce and Industry. (2005). The Economic Effects of Terrorism on London - Experiences of Firms in London's Business Community London.
Mäki, U. (1992). On the Method of Isolation in Economics. *Poznan Studies in the Philosophy of the Sciences and the Humanities, 38*, 147–168.
Osborne, M. J., & Rubinstein, A. (1994). *A Course in Game Theory*. Cambridge: The MIT Press.
Petropouleas, I. D. (2009). Protecting Buildings and Infrastructure Against Acts of Terrorism. Paper.
Phillips, C. (2010). UK CT Strategy to protect crowded places. In NaCTSO (Ed.), *Counter Terror Expo 2010. Protecting Crowded Places Against Terrorism*. National Hall, Olympia.
Powell, R. (2007a). Allocating Defensive Resources with Private Information about Vulnerability. *American Political Science Review, 101*, 799–809.
Powell, R. (2007b). Defending against Terrorist Attacks with Limited Resources. *American Political Science Review, 101*, 527–541.
Powell, R. (2008). Allocating Defensive Resources Prior to Attack. *ISA's 49th Annual Convention, Bridging Multiple Divides* San Francisco: International Studies Association.
Rubin, G. J., Brewin, C. R., Greenberg, N., Hughes, J. H., Simpson, J., & Wessely, S. (2007). Enduring consequences of terrorism: 7-month follow-up survey of reactions to the bombings in London on 7 July 2005. *The British Journal of Psychiatry, 190*, 350–356.
Rubinstein, A. (2006). Dilemmas of an Economic Theorist. *Econometrica, 74*, 865–883.
Sandler, T., & Lapan, H. E. (1988). The calculus of dissent: An analysis of terrorists' choice of targets. *Synthese, 76*, 245–261.
Snidal, D. (2004). Formal Models of International Politics. In D. F. Sprintz & Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases. Methods for Studying International Relations*. Ann Arbor: The University of Michigan Press.
Sugden, R. (2000). Credible worlds: the status of theoretical models in economics. *Journal of Economic Methodology, 7*, 1–31.
The Stationary, O. (2006). Report of the Official Account of the Bombings in London on 7th July 2005. London: The Stationary Office.
Transport for London. (2005a). 06.40 hours - Tube services today. (Vol. 2010). London: Transport for London.
Transport for London. (2005b). 15:15 - Transport for London Update. (Vol. 2010). London: Transport for London.

Transport for London. (2005c). Tube passenger numbers showing strong recovery. (Vol. 2010). London: Transport for London.

Paper 1

"Aiming for Mass Killings: Modelling Terrorists' Selection of Targets".

Paper 2

"Preventing mass killings: Determining the optimal allocation of security resources between crowded targets", published in *Peace Economics, Peace Science and Public Policy*.

Paper 3

"Reducing Harm from Explosive Attacks against Railways", published in *Security Journal*.

Paper 4

(with Paul Ekblom) “Specifying the explosion-resistant railway carriage - a desktop test of the Security Function Framework”, published in *Journal of Transportation Security*.

Specifying the explosion-resistant railway carriage - a desktop test of the Security Function Framework[1]

Abstract

Anyone trying to devise counter-terrorist designs for railway carriages faces a range of issues. In particular, designers need a framework for thinking about security. This paper explores the specific practical design problem of securing railway carriages against explosive terrorist attacks and assesses the benefits of articulating such exploration through the use of the Security Function Framework (SFF). We present the SFF framework, apply it to the ExRes carriage and evaluate it according to defined criteria. Our evaluation shows that the SFF framework is clearly expressed, aids the designer in communicating design requirements, facilitates systematic creativity without necessarily generating completely new ideas, and appears practically applicable. However, we emphasize that ours have been 'bench tests'; such tests are really no substitute for trying the SFF out with real life designers.

Key words: Security, Design against Crime, Offender Scripts, Counter-terrorism, Transport, Improvised Explosive Devices.

[1] Sunniva Meyer thanks Institute of Transport Economics and the Research Council of Norway for funding her contribution to this study.

1. Introduction

Railway sites are attractive targets for terrorists: they are both crowded and easily accessible, and offer the prospect of highly-disruptive and high-profile outcomes. Several of the deadliest attacks in European history have actually targeted passenger traffic on railways (Lia and Nesser 2005: 37–38). Attack methods range from derailing (e.g. the attempted derailing of the high-speed railway between Madrid and Seville in 2004) to poison gas (Japan) to suicide bombing (London). Explosive attacks are particularly attractive; they can damage structures and bring down buildings, as well as kill people. Furthermore, media coverage of bombings is considerably more graphic than coverage of, say, a shooting (Clarke and Newman 2006: 109). This paper thus focuses on attacks using explosives, whether carried onto the train by pedestrians or vehicle-borne at the trackside, and whether suicidal or not.

Terrorism has diverse causes at many levels (Roach et al. 2005), and correspondingly many kinds of intervention exist. Situational crime prevention (e.g. Clarke and Newman (2006)) works through increasing the (real and perceived) risk and effort of committing terrorist acts, and reducing the reward, by changing the targets and environments of terrorism and influencing the behaviour of preventive agents such as guardians and place managers. One sector which can contribute to situational prevention is the industrial design, construction and manufacture of places and products. A specific domain within this sector is the design and construction of railway carriages. The first purpose of this paper is to explore the specific practical problem of designing explosion-resistant railway carriages.

Anyone trying to devise counter-terrorist designs for railway carriages faces a range of issues. For example, the designs must be effective, and they must minimally interfere with everyday running of the railway or passenger safety, comfort and convenience. The designs must also be implementable, whether in terms of practical/technological constraints on manufacture, or in terms of appeal and feasibility to the diverse decision-makers. In the complex, privatised world of railways (Design Council 2000) responsibility is divided (in the UK for example) between train operating companies, rolling stock hire companies (who own the

carriages and rent them to operators), carriage designers and builders, and the track provider (National Rail).

In this context it is easy for designers to become confused. To help designers build their capacity to innovate and communicate, a language and framework of security is needed. Such a framework should articulate the requirements of security, integrating these requirements with all the other aspects of design[2]. The second purpose of this paper is thus to assess the benefits of a particular language and framework, the Security Function Framework (SFF), which has been developed in a very different context, covering the design of secure bike parking facilities (Thorpe et al. 2009) and of anti-theft clips to secure customers' bags to tables in bars (Ekblom 2012 a,b).

What requirements should a security framework fulfil? Drawing on Cropley's (2010)) functional treatment of creativity, it should support the generation of designs that are effective and relevant, novel and surprising, elegant and generalisable. It should be deliberative in fostering close and careful attention to detail. It should also be systematic and rigorous, supportive of use of research evidence and theory. It should be practical in leading from theory and research to the design of real working products, places and systems.

The rest of the paper proceeds as follows. Section 2 describes how the value-added contribution of a security framework might be assessed. Section 3 introduces the SFF. Section 4 applies the SFF to explosion-resistant carriages, leading to an analysis of the problem and a design specification for solutions. Section 5 assesses the SFF as a means of generating good design specifications with regard to its application and, finally, section 6 summarizes this paper.

[2] Most of these will be ordinary, everyday needs such as safety, economy and convenience. In a peacetime society where armoured trains are historical or cinematic freaks, civil needs should predominate – we should avoid 'vulnerability-led' designs (Durodié 2002) and 'paranoid products' (Gamman and Thorpe 2007). To do otherwise would be to concede a victory to the terrorists.

2. Assessment criteria

As stated in the introduction, assessment can cover both the ExRes design specification we have produced, and the performance of the SFF in generating that specification. In both cases an ideal approach, would include trying out the specification and the framework on real designers (neither of us are practising industrial designers, although one of us regularly works with them), and preferably those designers from the rail industry. But for reasons now to become apparent, these aspirations are some way down the line.

Assessing the ExRes Carriage

How might we evaluate the ExRes Carriage specification? Obviously we cannot yet assess the quality and the performance of any real-world prototypes or production models that the specification has engendered, or even the range and variety of possibilities generated, since none has yet been constructed. Nor, for the same reason, can we assess the final technical design realisation as it might appear in Computer-Aided Design (for example using 'walk-through, think terrorist' exercises based on a virtual reality simulation of a carriage interior; or a computerised simulation of blast effects).

At the very least we can, as designers say, 'correlate' the final specification in terms of the original purpose-level requirement, with the suggestions for intervention mechanisms and methods that we have suggested: do the suggestions reflect the purpose? We can also correlate the specification with the theory and evidence of situational prevention, to see how plausible the elements of that specification are. We can also offer the specification for criticism to those (such as transport police) responsible for rail security or counter-terrorism and (one hopes) possessed of a wealth of practical experience, as described in the 'critique' stage of the Design Against Crime methodology.[3] In this way the rationale of the design can be subjected to scrutiny, if not strictly put to the test.

[3] www.designagainstcrime.com/?page_id=23

Assessing SFF

We're perhaps in a better position to assess the performance of SFF in helping to generate and communicate design specifications in a domain (counter-terrorist design in a large-scale product and extremely large-scale system), far from its origins in addressing everyday crimes through small-scale interventions, although here we have only a single case study, and again this is a self-assessment. Criteria for this assessment are that the SFF framework should be:

- clearly expressed,
- fertile, and
- practically applicable.

We offer some answers in section 5, drawing particularly on the experience of one of us who was a newcomer to SFF. Further answers cannot be given until we have a suite of case studies of specification generations, leading to actual design realisations and drawing on the experience of designers.

3. The Security Function Framework

Here we introduce a four-level framework, under development by Ekblom and colleagues (e.g. Ekblom 2009; Ekblom 2010; Ekblom 2012a, b) for describing a product's 'security function'. 'Security function' is taken to mean:

> The properties of a product which, interacting through causal mechanisms with entities, agents and systems within its environment, serve the purpose of reducing the risk of crime and increasing security and community safety. The properties in question may be deliberately conferred, amplified or directed through the design, materials and construction of the product and/or its environment. Risk is taken to include possibility of particular kinds of adverse events occurring, their probability and the harm they may cause.

The four-level framework consists of:

1. The product's *purpose*;
2. The product's *security niche*;
3. The product's *mechanisms*;
4. The *technical* description of the product.

Describing *purpose* covers several distinct aspects.

(I) What is the designed product *for?* This is its *principal* purpose. But this isn't the end of the story.

(II) What, if any, *subsidiary* purpose/s does it have? When the principal purpose doesn't relate to security, the security purpose may be a subsidiary one. We could take this further by considering each aspect of risk separately (is the purpose to eliminate the possibility of certain kinds of criminal event? Reduce the probability? Reduce the harm?). We should also specify where the product is intended to be used.

(III) What other *desire* requirements must it meet, that are beneficial to the immediate users and manufacturers; expressed alternatively, what other drivers must it satisfy?

(IV) Finally, what '*hygiene'* or *social responsibility* requirements must it meet, referring to other societal values which the product should not interfere with, or should positively boost?

In generic terms, the designer's major task in preventing crime is to identify and resolve the contradictions in the design requirement, whether these contradictions are strategic ones relating to fundamentals of the crime problem (keep passengers and property safe whilst maintaining an efficient, attractive and economic rail service), or tactical ones which may relate to 'troublesome tradeoffs (Ekblom 2005) with other drivers/values (such as energy efficiency or social inclusion) or within crime prevention itself. Contradictions apart, the designer must also seek to exploit complementary or synergistic functions.

The concept of *security niche* attempts to characterise how the security function within a given product relates to other products, people and places in the human ecosystem.

Consider some product, such as a handbag or laptop carrier, which is at risk of being a target of, or a tool for, crime. Security can be conferred in several ways, singly or in combination (cf Ekblom 2005):

- The bag could be *safe* – not in itself needing explicit security because it is used only in *secure environments*, protected by enclosures and/or people acting as crime preventers such as guardians or place managers (Clarke and Eck 2003). In practice complete safety occurs only in relatively rare circumstances.
- A bag that was in fact *exposed* to significant risk could be protected by separate *security products* or *securing products.* A security product's principal purpose is protecting some other target, person or property against crime – an example could be an audible alarm lanyard that is triggered if the bag is snatched. Secur*ing* products by contrast have a *subsidiary* security purpose additional to their principal purpose (for example the *Stop Thief* chair www.stopthiefchair.com/ is primarily for sitting on but a pair of notches cut in the front of the seat enables a bag to be securely hitched beneath the owner's knees, in a café or pub).
- Deploying the above approaches makes for a *secured product,* protected by external means. But the product itself could be designed to be a *secure* one, that protects itself:
    - by the incorporation of *security or securing components*. These components may either be retrofitted, or factory-fitted, where product and component are designed or selected to fit one another well, such as the tamper-evident lid on food containers. In the case of the bag, an RFID chip could be inserted to protect against shoplifting; since this chip could also help with stock control and supply chain monitoring, the RFID would be a securing product.

- by deliberate *security adaptations* (Ekblom and Sidebottom 2007) to its inherent causal properties, realised through constructional features and/or materials. These adaptations either work by themselves (such as anti-slash wire mesh incorporated within the fabric), or in conjunction with human action such as guardianship (for example where the opening flap of a handbag is fastened by Velcro, which alerts the owner by movement and noise when it is opened). Both these features and more are incorporated within the Karrysafe range designed by Adam Thorpe (www.inthebag.org.uk/?page_id=479).

The same product can occupy multiple niches and have several ecological relationships. In security terms this is captured in a distinction noted in Ekblom (2009) between a product as *object* of crime – an asset – and the same product *in-function*. Our bag can be stolen for its *own value*, as well as for the *contents* it contains and perhaps protects (as a securing product itself) valuables or fails to protect.

Purpose must ultimately link to more practical aspects of design. But it is best not to leap straight from high-level purpose to a technical specification as described below. Rather, smarter understanding (and more efficient knowledge transfer to other design tasks) requires an intermediate consideration of the causal *mechanisms – how* the design intervention works by interrupting, diverting or weakening those causes. Usually it is possible to identify several parallel mechanisms which may underlie a preventive effect (for example, physical blocking of crime, in parallel to subjective discouragement of offenders from anticipated effort). An understanding of immediate causal mechanisms of crime and its prevention is the royal road to analysing risk and reducing this risk through design. More generally, it is fundamental to replicating the core principles of successful crime prevention in ways that are intelligently and perhaps innovatively customised to new contexts (Pawson and Tilley 1997; Ekblom 2005).

Given that offenders can be seen as both ‘caused’ and as active, goal-directed, planning and decision-making agents (Ekblom 2007; Ekblom 2011), or ‘caused

agents' for short, a useful parallel perspective to straight causal mechanisms is that of *scripts* (Cornish 1994)(Freilich and Chermak 2009), supplemented by knowledge of offenders' perpetrator techniques (or modus operandi) and their *resources* (Ekblom and Tilley 2000; Gill 2005). For example, the offender has to seek a crime target (say a handbag), see and select the target, approach without arousing suspicion, steal the bag and escape preferably un-noticed, before converting and/or enjoying the value of the loot and perhaps covering tracks. Ekblom (2012b) extends this in design terms to the concept of *script clashes* – where the offender's script engages with the user or preventer's script in such issues as surveillance versus concealment, challenge versus excuse, pursuit versus escape. These clashes are, as it were, the pivots on which designers and other professional crime preventers have to tip the design of products, environments and procedures in favour of the good party. As offenders and preventers get to know and anticipate one another's' scripts and the mutual script clashes, the scripts may *co-evolve* towards greater elaboration of countermove and counter-countermove.

Technical descriptions state how the causal properties of the product, properties which contribute to the mechanisms of prevention described above, are realised through construction, manufacture and operation. *Construction* is about materials and distinguishable structural features of the design. *Manufacture* is about how it is made. *Operation* is about how it acts in tangible terms with human action (or conceivably, under control of artificial intelligence) such as keys turned, cards swiped or actuators releasing locks.

Four-level description – overview

In sum, an abbreviated four-level description of a security function could say something like this, using the Stop Thief chair as example:

> **1** (**purpose**) The Stop Thief chair is designed with principal purpose to serve as a fully functional and appropriately-styled chair, and subsidiary purpose – without in any way jeopardising the principal purpose – to reduce the risk of *theft* of *customers' bags* in places like *bars and restaurants*. **2** (**security niche**) It is thus a *securing product*. **3 (mechanism)** It works by supplying physical *anchorage* of the target bag, that is differentially easier to release by the bag-owner; by mobilising *usage of the security function of the chair,* and the *surveillance and reaction* that it favours by the user/owner and others acting as preventers; and by *deterrence* through increasing the offender's perception of risk of being detected and caught in the act. All these mechanisms are supported **4** (**technically**) by the incorporation of a *twin notch feature* cut or moulded in the leading edge of the seat part of the chair, over which the bag handle is placed by the user/owner, the bag then being anchored due to its handle being enclosed between the seat and the back of the user/owner's knees.

The complete description of the design of secure or securing products in particular must of course go well beyond security and crime considerations. How the design satisfies other purposes and requirements, perhaps resolving troublesome tradeoffs between security and desire factors such as convenience, safety, economy and style, are all key to the wider design process. If all these requirements are inadequately addressed, then there is little point in getting the crime prevention requirement right because nobody will buy the chair! Similarly, if the consequences of *poor* security design are that fewer people buy the chair, then sales will be lower and that will have commercial repercussions; but experience has suggested that *good* design can give this concept a Unique Selling Proposition.

4. The ExRes carriage

Having developed the SFF in the context of everyday crimes and modest design interventions, how does it fare when handling design against extreme and rare crimes against which radical interventions have been contemplated and sometimes implemented? This section tests out the Security Function Framework just introduced, to describe a suggested specification for an explosion-resistant railway carriage; the ExRes carriage.

The ExRes carriage's purpose

The principal purpose of the ExRes carriage is, obviously enough, to transport the passengers from one station to another.

The subsidiary, security, purpose is to protect passengers against injuries from explosive attacks by (1) decreasing the probability of anyone committing an explosive attack (*primary security*[4]); (2) decreasing the probability of an attack's being successful (*primary security*); and (3) decreasing the harm, intended or otherwise, inflicted by an explosive attack (*secondary security*[5]). It helps at this point to switch to the perspective of the offender. Assuming that the offender wants to maximize the expected harm[6] of an explosive attack *while* minimizing the cost of attacking, the probability of a possible offender committing an explosive attack depends on the offender's perceptions of the probability of an attack's being successful, the harm inflicted by an explosive attack and the cost of attacking[7,8].

---

[4] *Primary security* includes actions that eliminate *possibility* of criminal event (e.g. using system design to replace the annual payment of vehicle tax, which many drivers manage to evade, by increased fuel tax, which they cannot); or if this cannot be done, actions reduce its *probability* (e.g. making it harder to break into cars).

[5] *Secondary security* – if event does happen, action *limits harm to all parties and property as it unfolds* (e.g. stopping the ongoing damage and continued loss of revenue from a vandalised vending machine by rapidly alerting the repair team).

[6] What sort of harm he or she wants to maximize depends on the motivation behind the attack.

[7] See Meyer (2011) for a more elaborate explanation.

The ExRes Carriage must furthermore have some other *desire* qualities. The passenger wants it to be aesthetic, comfortable, safe and easy to enter/exit. The railway operator wants it to be economical to purchase, service and operate, safe, aesthetic, easy to clean, durable, easy to operate, spacious and appealing to passengers (including feeling safe). The manufacturer wants it to be relatively inexpensive to produce, suitable for a wide range of railway systems and safe for passengers (at least to the extent that the manufacturer might be liable should an event happen; more generously speaking, motivated by broader ethical considerations).

In addition, the ExRes carriage should meet some 'hygiene' or social responsibility requirements: it should be environmentally sustainable, energy effective, inclusive etc. As with cars, there is also a major concern with fail-safe and safety in crashes, some of which may synergise or conflict with anti-explosion requirements.

The ExRes carriage's security niche

The ExRes carriage is a securing product: it has a *principal* purpose of safely and comfortably transporting passengers plus a *subsidiary* security purpose of protecting passengers against injury from explosive attacks whilst on board or adjacent to the carriage (for example on the platform or in another passing train).

As valued assets in themselves, ordinary railway carriages additionally need security against the possibility that *they*, and not just the *people* they contain, are the target of crime (such as vandalism or theft of fittings) or terrorism. This reflects the distinction noted in section 4 between a product as object of crime and product in-function. Altogether, then, carriages could take the following niches (examples are illustrative more than necessarily practical):

[8] When increasing the probability that an offender will be caught, the measure increases *tertiary security* – action *limits propagation of harm* that may occur post-event, as well as *primary security*.

(1) *Safe* if sited in a *secure environment* where all personnel and passengers with belongings were screened for explosives before entering the railway carriage and both sidings and running tracks enclosed by physical barriers with access control and/or guarded. Planting of dense spiny bushes like blackthorn (Prunus spinosa) alongside the track could hinder access to both pedestrian and Vehicle Borne explosives whilst improving aesthetics (these bushes would be securing 'products'). Anything approaching complete safety is of course unlikely but a certain minimally secure environment is needed if constructing and operating a railway is to be a feasible proposition[9].

(2) *Secured* if protected by

- separate *security products,* dedicated to minimizing harm from explosive attacks against the carriages – for example, a sniffer for detecting explosives that the train guard carries while inspecting tickets.
- separate *securing products,* minimizing harm from explosive attacks against the railway carriage as a sideline. – for example, the practice of having season or multi-use tickets carrying personal identification, principally for revenue protection, could increase the risks to the offender.

(3) *Secure* if protected by

- *security* or *securing components*, for example if a warning system for suspicious behaviour or vapours were installed in the railway carriages.
- deliberate *security adaptations*, for example if carriage walls were made of blast-absorbing materials.

[9] As with so-called 'pacification' of Native Americans in the 19th-Century West or theft of copper signal cabling in the UK today (Sidebottom et al. in press).

The securing function of the carriage, protecting the passengers it conveys, is conferred by (2) and (3) above.

Mechanisms

To design a railway carriage that protects passengers against injuries from explosive attacks we must understand the immediate causal mechanisms that allow those attacks to take place; and thus how these causal mechanisms can be interrupted such that the passengers' injuries are avoided or minimized in case of an explosive attack. As mentioned earlier, injuries can be minimized by (1) reducing the probability of anyone attempting an explosive attack; (2) reducing the probability of an attack's being successful; and (3) reducing the harm inflicted by an explosive attack. The probability of a possible offender attempting an explosive attack depends on the offenders' perceptions of the probability of an attack's being successful, the harm inflicted by an explosive attack and the cost of attacking given that the offender wants to maximize harm and minimize the cost of attacking.

Visualising dynamic mechanisms requires considering scripts and perpetrator techniques. When targeting a railway carriage, an explosive device can be delivered either by backpack/suitcase/shopping bag (person borne), or by car/truck (vehicle borne). A person borne explosive can be left to detonate, inside a carriage by a passenger/employee or on the rail track, or detonated while carried, i.e. suicide attack (Meyer 2011). Some abbreviated examples follow. A crime script[10] for an offender when leaving a device inside a railway carriage could go something like this:

1. Enter station *without* being detected or challenged.
2. Wait for suitable railway carriage *while* keeping the explosives safe from weather or accidental premature detonation.
3. Enter railway carriage *while* keeping the explosives safe from weather or accidental premature detonation.

[10] All crime scripts in this function statement obviously assume that necessary reconnaissance, explosive and tool purchases and device assembling already have been accomplished.

4. Search for suitable hiding place *while* keeping the explosives safe from weather or accidental premature detonation and *without* being spotted or challenged.
5. Leave container with explosive at hiding place *without* being spotted or challenged.
6. Exit carriage *without* being challenged.
7. Leave station *without* being challenged.
8. Detonate explosive if it is remote controlled (and without automatic timer) *without* being spotted and frustrated, or (for bombers who wish to survive) getting injured from the explosion.

A crime script for an offender when leaving an explosive on the railway track could be:

1. Search for unguarded entrance to tracks, or create one by cutting fence.
2. Enter tracks through unguarded entrance *without* being spotted or challenged.
3. Search for suitable spot to leave explosive *without* being run down by train.
4. Leave explosive at suitable spot *without* being spotted.
5. Exit tracks through unguarded entrance *without* being spotted or challenged.
6. Leave site before railway carriage hits the explosive(s) *without* being spotted.

A crime script for a person borne suicide attack could be:

1. Enter station *without* being spotted or challenged.
2. Wait for suitable railway carriage *while* keeping the explosives safe from weather or accidental premature detonation.
3. Enter railway carriage *while* keeping explosives safe from weather or accidental premature detonation.
4. Sit down or stand in carriage *while* keeping explosives safe from accidental premature detonation.
5. Wait for suitable moment in terms of crowded carriage, location in tunnel or high-visibility place (e.g. on a bridge) and detonate explosives.

A person borne explosive is limited by the weight an individual can carry, while a vehicle borne explosive can obviously be much larger. A vehicle can be parked along the track or crashed into the carriage. The crime script for an offender parking a vehicle along or, if possible, on the track might be:

1. Find suitable spot for the explosive(s) and for nearby viewing point for detonation *without* being spotted or challenged.
2. Remove any physical obstacles at detonation site *without* being spotted or challenged.
3. Arm device and leave vehicle *without* being spotted or challenged.
4. Leave area and/or go to viewing point.
5. Detonate device if remote controlled *without* being spotted or getting injured from explosion.

The crime script for an offender crashing into a railway carriage with a vehicle borne explosive could be:

1. Find suitable spot for crashing vehicle into carriage *without* being spotted or challenged.
2. Remove any physical obstacles *without* being spotted or challenged.
3. Arm device and await train *without* being spotted or challenged.
4. Crash into carriage *while* detonating the explosives.

The passenger script is:

1. Enter station.
2. Wait for train *while* keeping comfortable.
3. Enter railway carriage.
4. Sit down or find place to stand.
5. Wait for right station, with or without entertainment, or other mental strategies for occupying time and/or shutting out what may be noisy, crowded surroundings.
6. Exit railway carriage.
7. Exit station.

The employee script would vary with work tasks, but may include looking out for suspicious behaviour and left-behind items.

Script clashes here include

- surveillance by employees versus offender hiding explosives in carriage or on track
- surveillance by passengers versus offender hiding explosives in carriage
- driver stopping train if spotting vehicle or explosive device on the track

Applying the above scripts, the following mechanisms for *minimizing passenger injuries* from *explosive attacks* against railway carriages can be distinguished:

- One way of decreasing the probability (and the offender's perception of the probability) of an attack with explosives left inside carriage's being successful is to *minimize the number of forgotten items*: if the design prevents people from forgetting items, a left-behind object will be more suspicious and, accordingly, more resources will be available to investigate whether the left object might be an explosive. It should also be easy for passengers to spot their own forgotten luggage when leaving their seat.
- A second way to decrease the probability (and the offender's perception of the probability) that an attack with explosives left inside the carriage is successful is to maximize the ability to spot any left item: if the left item is spotted, passengers can alert employees and the employees might thus implement suitable responses. Accordingly, the carriage should be designed with no hiding places and it should be easy surveillable.

- A third way to decrease the probability (and the offender's perception of the probability) that an attack with explosives inside the carriage is successful is installing explosive detectors at the entrances. An explosives detector is "a device capable of detecting the presence of certain types of explosives" (Garcia 2008: 331). The current technology is, however, too space demanding

(and perhaps also too people intensive) to make it a viable option for now. Cost and speed of the current technology also makes the option less viable[11].

The offender's perception of his/her cost of attacking depends on his perception of the probability of being caught: if an explosive attack is committed by leaving an explosive device on site, the preventers' capability of identifying the offender increases the cost of attacking. CCTV can help solve this problem [The fact that in-carriage CCTV has been deployed to prevent conventional crimes and antisocial behaviour gives a 'free ride' to the anti-terrorist function].

Whether an explosive is left before detonation or the offender commits a suicide attack, it is desirable to minimize the harm inflicted from an explosive detonated inside the carriage. One way of doing this is to minimize injuries from (secondary) fragments. Other ways of minimizing human injuries are to reduce the internal blast and use materials that do not ignite in an explosion or in a fire.

In addition to protecting the passengers from an internal blast, the carriage ideally should be constructed to withstand external blasts. Current technology, however, can only strengthen a carriage structure to withstand small charges or detonations at some distance; making a carriage able to withstand a vehicle borne explosive crashing into the carriage is not feasible.

To summarise preventive mechanisms, the ExRes carriage should be specified to *minimize passenger injuries* from *explosives* by (1) minimizing the number of forgotten items; (2) maximizing the surveillability of the carriage; (3) increasing the offender's perception of the probability of being caught; (4) preventing injuries from fragments; (5) aiming for a design which absorbs the blast energy from explosives detonated internally; and (6) strengthening the carriage structure to withstand an externally generated blast (only realistic for small charges or detonations at some distance). There may be additional requirements and assumptions about the security of the operating environment that these requirements for the carriage have to dovetail with.

[11] See explosive-sniffing ticket barriers at www.telegraph.co.uk/news/worldnews/asia/japan/7305856/New-Tokyo-train-barriers-test-passengers-for-explosives.html

The designers would of course have to simultaneously consider all the other, *non*-terrorism requirements of the carriage in its principal function as a conveyance, as previously described.

Technicalities

Describing the technicalities is primarily the designers' and engineers' task – where they exercise their skill, discipline and creativity to develop, through various iteration-and-test procedures,[12] and practical renditions of requirements such as those set out above. Indeed, stating requirements in such a way as to maximise design freedom is important not just as a general principle of industrial design but as a specific strategy to keep ahead of adaptive terrorists (Ekblom 2005, 2008). This usually relates to 'performance standards' rather than 'construction standards'.

In developing technical solutions designers would need to be able to state how the causal properties of their design of carriage (in conjunction with influences from passengers, luggage, bomb etc) realised each preventive mechanism in terms of materials, structure, operation etc, without interfering with the other requirements (and maybe actually synergising with them). They would also have to give an account in terms of blocking offender scripts and biasing script clashes to favour preventers. There is also the crime-specific possibility of design contradictions *within* the security requirements – for example, bigger windows to facilitate surveillance may weaken blast-resistance. In fact, from the designers' perspective, clearly-stated contradictions serve to sharpen and orientate their thinking (Ekblom 2008).

Some general guidelines may be distinguished from the above discussion[13]:

The number of forgotten items might be minimized by removing storage areas, especially areas where it is not evident who owns the luggage like for example shelf

[12] e.g. see www.designagainstcrime.com/methodology-resources/design-methodology/#users-abusers

[13] The overview in this section is on the concept level. The feasibility of any technical solution must be evaluated through simulation or testing.

areas close to the entrances. Ideally, the passengers should keep their luggage on their lap or between their feet (if small and light) or close by in their 'personal space' (if bulky or heavy). The seats should be formed in such a way that anyone leaving their seat plus fellow passengers should immediately spot any left item. Ideally all seats should face some other seat to maximize passenger surveillance. Design contradictions include removing storage areas versus supporting accessibility and comfort. For instance, absence of areas to put luggage might force passengers to leave it in the walkway such that it hinders movement through the carriage. Absence of shelving might also force passengers to keep luggage on the lap and thus decrease their comfort. Reducing the number of forgotten items can also have positive externalities; forgotten items can cause false alarms which also can reduce passengers' feeling of safety and disrupt services, both of which could deter passengers from train travel.

The surveillability of the carriage can be maximized by removing all unnecessary clutter and designing seats and other interior that does not hinder sight more than necessary. (Unfortunately, the rush-hour crowding that is so attractive to terrorists for boosting their kill, also serves to block this technique.) Interior walls should be transparent and seats designed so they do not unnecessarily decrease surveillability. Rubbish bins should ideally be removed (some operators have a rubbish collecting service during the journey) or made blast-resistant (which is very expensive). Hiding places should be designed out. An important contradiction is minimizing litter bins versus passenger comfort. A shortage of bins might cause passengers to throw their litter on the floor and, accordingly, decrease cleanliness. A possible solution is to increase the frequency of cleaning, but that would also lead to increased operating costs.

The offender's perception of the probability of being caught after the event (if still alive) might be increased by installing CCTV and/or dummy CCTV at all carriage entrances – all entrances must appear to be under surveillance or the offender would just avoid the unmonitored entrances. The real CCTV-cameras should store all pictures and have a high enough picture quality to enable identity recognition of offenders. The CCTV coverage should either be immediately stored at an external

server or the storing unit needs to be blast resistant. Installing high quality CCTV would however probably increase both the production costs and the operating costs drastically. Passenger privacy would also suffer with high density of CCTV coverage.

Injuries from fragments can be prevented by removing clutter that might be 'weaponised', turning into hazardous fragments in an explosion. Necessary interior structures, including glazing, should be blast-resistant or, at least, not form dangerous fragments in case of an explosion. This can be done by securing glass and using appropriate materials in the interior in an explosion. Internal sectioning might also hinder fragments from harming people over a large radius. High passenger density will, however, limit the circulation of fragments in itself (albeit unfortunately for those passengers nearest the blast).

Other ways of minimizing human injuries are to reduce the internal blast (to some extent) by ensuring rapid and sufficient ventilation of explosive gases, e.g through the windows and/or to use materials that do not ignite in an explosion or in a fire.

Injuries from explosives outside the carriage can be minimized by strengthening both carriage walls and carriage floors against external blasts. (Strengthening ribs to keep the compartment intact in case of derailment may confer some anti-blast or -ram benefit incidentally). Strengthening floors and walls might, however, increase the weight of the carriages and thus the energy consumed when moving the carriage. There is, furthermore, a tradeoff between securing against explosives from external and internal blasts; strengthened walls can hinder the ventilation of gases, increase the blast reflection and thus the injuries caused by an internal blasts. This is a contradiction to challenge designers' ingenuity.

In sum, the ExRes carriage's design should (1) minimize storage areas; (2) remove unnecessary clutter and only include interior that does not hinder surveillance more than necessary; (3) possibly install CCTV at entrances; (4) only include interior that resists fragmentation and fire; (5) ensure rapid and sufficient ventilation of explosive gases; and (6) strengthen carriage walls and floors.

Summary of SFF description

The abbreviated four-level description of the security function of the ExRes carriage specification translates to:

> **1** (**Purpose**) The ExRes carriage is specified with principal purpose to serve as a fully functional and appropriately-adapted railway carriage, and subsidiary purpose to *minimize passenger injuries* from *explosives* detonated either inside or outside of the carriage.
>
> **2** (**Security niche**) ExRes is above all a *securing* product: its security function is subsidiary to its principal purpose as a conveyance. As an asset to be protected in itself it is also a *secured* product to the extent it has security conferred by external means linked to the carriage and the people within it; and a *secure* product to the extent that it is designed and constructed to prevent and resist damage. It is only to a very limited extent a *safe* product given the difficulty of creating a secure environment around a target as geographically extended, complex and accessible to users as the railway.
>
> **3 (Mechanism)** The security function of ExRes is realised by (1) minimizing the number of forgotten items; (2) maximizing the surveillability of the carriage; (3) increasing the offender's perception of the probability of being caught; (4) preventing injuries from fragments; (5) absorbing the blast energy from explosives detonated internally; and (6) strengthening the carriage structure such that it can withstand an externally generated blast and thus minimize passenger injuries (only realistic for small charges or detonations at some distance).
>
> **4** (**Technically**)These mechanisms may be realised by (1) minimizing storage areas; (2) removing unnecessary clutter and only including interior that does not hinder sight more than necessary; (3) installing CCTV at entrances; (4) only including interior that resist fragmentation and fire; (5) ensuring rapid and sufficient ventilation of explosive gases; and (6) strengthening carriage walls and floors.

5. Assessing the framework

Section 3 formulated three criteria for the SFF framework: it should be (1) clearly expressed, (2) fertile and (3) practically applicable. This section attempts to assess the framework's performance on paper with regard to these criteria.

Clear expression

Clear expression; requires that SFF should articulate the design problem so as to facilitate communication, knowledge transfer and accumulation. It should thus only use terms that (1) are easily accessible to all SFF framework users regardless of field of expertise and (2) have unambiguous meanings such that all users interpret the terms similarly. When introducing new terms, the framework must include appropriate guidance on definitions. We include this criterion since each product description should be read with a single meaning, and no ambiguity.

The SFF framework description in section 4 does include clear definitions of the terms used, facilitating easier use of the framework. It furthermore distinguishes between the different aspects of the product's purpose and thus forces the designer to make explicit all the purposes the product needs to fulfil. In the example of the ExRes carriage, the SFF framework highlights the carriage's security purpose while also emphasizing that the carriage's main purpose is to transport passengers. The SFF framework furthermore introduces the term *security niche* to force the designer to formulate how a given product relates to other products, people and places with a security function. In the description of the ExRes carriage, the framework shows how the ExRes carriage both can be protected as a valued asset and protect people. The SFF framework also makes explicit the mechanisms that increase security and helps aids the designer in clearly expressing product requirements.

Hence, the SFF framework is both clearly expressed and aids the designer in communicating the design requirements.

Fertile

The second criterion requires that the SFF framework is *fertile*: it should maximise design freedom and creativity so as to facilitate production of new ideas, ideally even innovative, ideas which can solve real-world security problems, help out-innovate adaptive criminals, and keep up with social and technological change. The ideas generated should also be quite plausible and/or assist the designer in filtering out ideas with flaws. We include this criterion since we want the SFF framework to support the making of new solutions that enhance security.

The emphasis on mechanisms in the SFF framework aids the designer in thinking through different ways of increasing security, systematically pairing old ideas and combining them to form new ideas, and thus fosters creativity. However, have any completely new ideas been developed through this exercise? The authors do not have full overview over which ideas has been developed for enhancing security in carriages. We do, however, know that maximizing surveillability, preventing injuries from fragments and increasing structural redundancy have elsewhere been used to secure *buildings* against explosives. In rail transport public address messages about keeping belongings close, increased CCTV-coverage and increased presence of security personnel have been employed, all which can be interpreted as strategies to minimize number of forgotten items and increasing the offender's perception of the probability of being caught. We have thus no reason to believe that this exercise has resulted in any revolutionary new ideas.

Hence, the SFF framework may facilitate structured creativity rather than fostering completely new ideas. A new award-winning idea would probably depend more on a designer's creativity and posing questions from unusual and original angles than a specific framework. But for designers both highly creative and less creative, the SFF framework would at least tell them where to focus their thoughts.

Practical applicability

The third criterion requires that the SFF framework is *practically applicable*; it should systematically facilitate spelling out all facets necessary before designing the product. It should thus (1) make strong links from purpose to practical product, (2) systematically cover an appropriately-wide range of requirements and possibilities, and (3) highlight design contradictions, tradeoffs and context-dependencies. We include this criterion because we want the SFF framework to contribute to the making of physical objects in the messy and complicated real world rather than abstract ideas.

This criterion is difficult to evaluate with regard to the ExRes carriage since no designers have endeavoured to realize the specification and no prototype has been made. However, the SFF framework facilitates exploring design contradictions when discussing technicalities. In the ExRes carriage example, the design contradictions of removing storage versus supporting accessibility and comfort and minimizing litter bins versus passenger comfort are brought to attention. The SFF framework has furthermore been developed in contexts where prototypes *have* been developed; secure bike parking facilities and anti-theft clips to secure customers' bags to tables in bars.

Hence, the SFF framework seemingly is quite practically applicable.

Summary of self-assessment

In sum, the SFF framework is clearly expressed and thus aids the designer in communicating the design requirements, facilitates systematic creativity without necessarily generating completely new ideas and seems practically applicable. But these are 'bench tests' and there is really no substitute for trying the SFF framework out with real live designers.

6. Conclusion

Anyone trying to devise counter-terrorist designs in railway carriages (or anything else) faces a range of issues. To help designers through these processes and to build their capacity to innovate and communicate in this field, a framework of security is needed. The purpose of this paper was twofold: both to explore the specific practical problem of designing railway carriages against explosive attacks by terrorists; and to assess the benefits of articulating this exploration through the use of a particular language and framework, the Security Function Framework (SFF).

This paper has presented the SFF framework, applied it to the ExRes carriage and evaluated the SFF framework with regard to defined criteria. The evaluation shows that the SFF framework is clearly expressed and thus aids the designer in communicating the design requirements, facilitates systematic creativity without necessarily generating completely new ideas and seems practically applicable. But these have been ‘bench tests’ and there is really no substitute for trying the SFF framework out with real live designers.

References

Clarke, R., and Eck, J. (2003) *Become a Problem-Solving Crime Analyst in 55 small steps*. London: Jill Dando Institute of Security and Crime Science.

Clarke, R. and Newman, G. (2006) *Outsmarting the terrorists.* London: Praeger Security International.

Cornish, D. (1994) 'The Procedural Analysis of Offending and its Relevance for Situational Prevention.' *Crime Prevention Studies,* 3. Monsey, NY: Criminal Justice Press.

Cropley, D. (2010) 'The Dark Side of Creativity - A Differentiated Model' in Cropley, D., Cropley, A., Kaufman, J. and Runco, M. (eds) (2010) *The Dark Side of Creativity*. Cambridge: Cambridge University Press.

Design Council (2000) *Design Against Crime. A Report to the Design Council, The Home Office and the Department of Trade and Industry*. London: Design Council. Online. Available www.shu.ac.uk/schools/cs/cri/adrc/dac/designagainstcrimereport.pdf

Durodié, B. (2002) 'Perception and Threat: Why Vulnerability-Led Responses will Fail', *Homeland Security and Resilience Monitor*, 1:16–18.

Ekblom, P. (2005) 'Designing Products against Crime' in N. Tilley (ed.), *Handbook of Crime Prevention and Community Safety'.* Cullompton: Willan

Ekblom, P. (2008) 'Designing Products against Crime' in Wortley, R., Mazerolle, L. (eds) *Environmental criminology and crime analysis*. Cullompton: Willan.

Ekblom, P. (2009) *Standard generation through application of CCO framework*. Unpublished final report WPA2 of 'Bike Off 2 – Catalysing Anti Theft Bike, Bike Parking and Information Design for the 21st Century'. At www.bikeoff.org/2009/01/05/final-report-wpa2-of-bike-off-2/

Ekblom, P. (2010) 'How to understand, specify and describe the security function of a product: Towards a language and a framework for designing against crime', International Seminar on Environmental Criminology and Crime Analysis (ECCA), Brisbane.

Ekblom, P. (2011) *Crime Prevention, Security and Community Safety Using the 5Is Framework.* Basingstoke: Palgrave Macmillan.

Ekblom, P. (2012a) 'The Security Function Framework', in Ekblom, P. (ed) *Design against crime: crime proofing everyday objects.* Crime Prevention Studies 27. Lynne Rienner, Boulder, Col.

Ekblom, P. (2012b) ‘Happy returns: ideas brought back from situational crime prevention’s exploration of design against crime’, in Farrell, G., Tilley, N. (eds) *The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke*. Crime Science series. Willan, Cullompton.

Ekblom, P. (in preparation) ‘How to understand, specify and describe the security function of a product: towards a language and a framework for designing against crime’ in P. Ekblom (ed), *From Research to Realisation: Designing out Crime from products* Crime Prevention Studies. Boulder, Col.: Lynne Rienner.

Ekblom, P., Bowers, K., Gamman, L., Sidebottom, A., Thomas, C., Thorpe, A., Willcocks, M. (2012) ‘Reducing bag 676 theft in bars’, in Ekblom, P. (ed) *Design against crime: crime proofing everyday objects*.

Ekblom, P. and Sidebottom, A. (2007) ‘What do you mean, ‘Is it secure?’ Redesigning language to be fit for the task of assessing the security of domestic and personal electronic goods.’ European Journal on Criminal Policy and Research, 14: 61–87.

Ekblom, P. and Tilley, N. (2000). ‘Going Equipped: Criminology, Situational Crime Prevention and the Resourceful Offender’ *British Journal of Criminology* 40: 376–398.

Freilich, J. and Chermak, S. (2009) ‘Preventing Deadly Encounters between Law Enforcement and American Far-Rightists’ *Crime Prevention Studies* 25:141–172.

Gamman, L. and Thorpe, A. (2007) ‘Profit from Paranoia – Design Against 'Paranoid' Products.” Paper presented at European Academy of Design conference on Dancing with Disorder: Design, Discourse, Disaster. Izmir, Turkey. Online. www.bikeoff.org/2007/04/30/profit-from-paranoia-design-against-paranoid-products/

Garcia, M. (2008) *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann.

Gill, M. (2005) ‘Reducing the Capacity to Offend: Restricting Resources for Offending’ in Tilley, N. (ed) *Handbook of Crime Prevention and Community Safety.* Cullompton: Willan.

Lia, B. and Nesser, P. (2005) ‘Terror mot jarnvegar: Eit oversyn over typiske terroraksjonar mot togpassasjertransport.’ Kjeller: FFI.

Meyer, S. (2011) ‘Reducing Harm from Explosive Attacks against Railways’. *Security Journal.*

Pawson, R. and Tilley, N. (1997) *Realistic Evaluation*. London: Sage.

Roach, J, Ekblom, P and Flynn, R (2005) 'The Conjunction of Terrorist Opportunity: A Framework for Diagnosing and Preventing Acts of Terrorism.' *Security Journal* 18: 7–25.

Sidebottom, A., Belur, J., Bowers, K., Tompson, L. and Johnson, S. D. (in press). Theft in price-volatile markets: On the relationship between copper price and copper theft. Journal of Research in Crime and Delinquency.

Thorpe, A., Gamman, L., Ekblom, P., Johnson, S. and Sidebottom, A. (2009) 'Bike Off 2 – Catalysing Anti-Theft Bike, Bike Parking and Information Design for the 21st Century: an Open Innovation Research Approach', in T. Inns (ed.) *Designing for the 21st Century*: Volume 2. Interdisciplinary Methods and Findings.